North Korean APT group 'Kimsuky' targeting experts with new spearphishing campaign

By James Reddick

Published: 2023-03-22 · Archived: 2026-04-05 15:32:36 UTC

German and South Korean government agencies this week warned about a new spearphishing campaign from a notorious North Korean group targeting experts on the peninsula.

The campaign gains access to victims' Google accounts through two attack methods — the infection of Android phones through a malicious app on Google Play and the use of a malicious Chromium web browser extension.

The advanced persistent threat (APT) group — whose many names include TA406 and Thallium — has been in operation since 2012, largely targeting diplomats, non-governmental organizations, think tanks, and experts on issues related to the Korean peninsula.

The advisory, released Monday by Germany's Constitutional Protection Agency and the Republic of Korea's National Intelligence Service, describes a highly targeted campaign focusing on familiar victims.

"The National Intelligence Service and the Constitutional Protection Agency believe that the hacking attack described above is mainly targeting experts on the Korean Peninsula and North Korea, but since the technology exploited in this attack can be used universally, it can be used by foreign affairs and security think tanks around the world as well as unspecified people," they wrote.

As they have in previous campaigns, Kimsuky used spearphishing attacks to gain initial access "by impersonating portal administrators and acquaintances." In some cases, the emails induced an installation of a malicious extension on Chromium-based browsers, which was automatically enabled. When the victims open Gmail, the program steals the person's emails, which are sent to a server belonging to the attackers.

In another attack, Kimsuky actors add a malicious app to Google Play Console for "internal testing" and give permission to a targeted person to access it. After getting access to their login credentials in a spearphishing attack, they download the app through the victim's account, which is then synced to their Android smartphone.

According to the advisory, the actors stole both emails as well data stored in the cloud.

An October 2020 alert on the group from the United States Cybersecurity and Infrastructure Agency described Kimsuky as "likely tasked by the North Korean regime with a global intelligence gathering mission." In some cases, hackers posed as South Korean reporters to gain access to targets.

Recorded Future®

Know what matters.

Act first.

Get started

[James Reddick]

has worked as a journalist around the world, including in Lebanon and in Cambodia, where he was Deputy Managing Editor of The Phnom Penh Post. He is also a radio and podcast producer for outlets like Snap Judgment.

Source: https://therecord.media/north-korea-apt-kimsuky-attacks